

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named
Inventor : Arnaud Capitant et al.
Appln. No. : 09/332,489
Filed : June 14, 1999
Title : PROCESS FOR MAKING REMOTE PAYMENTS
FOR THE PURCHASE OF GOODS AND/OR A
SERVICE THROUGH A MOBILE
RADIOTELEPHONE, AND CORRESPONDING
SYSTEM AND MOBILE RADIOTELEPHONE
Docket No. : S828.312-0002



Group Art Unit: 2744
Examiner:

**CLAIM OF PRIORITY AND TRANSMITTAL OF
CERTIFIED COPY OF PRIORITY DOCUMENT**

Assistant Commissioner for Patents
Washington, D.C. 20231

I CERTIFY THAT THIS PAPER IS BEING SENT BY U.S. MAIL,
FIRST CLASS, TO THE ASSISTANT COMMISSIONER FOR
PATENTS, WASHINGTON, D.C. 20231, THIS 18th DAY OF

January 2000
PATENT ATTORNEY

Sir:

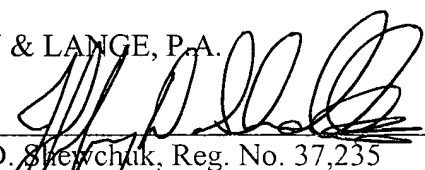
Applicant claims right of priority under the provisions of 35 U.S.C. 119(a)-(d) or 365(b) based on French Application No. 98.07666, filed June 15, 1998, and French Application No. 98 13471 filed October 23, 1998.

Certified copies of these applications are enclosed. These priority applications are identified in the Declarations filed January 18, 2000.

Applicant requests that priority be granted on the basis of these applications.

Respectfully submitted,

KINNEY & LANGE, P.A.

By: 
Jeffrey D. Stewchuk, Reg. No. 37,235
THE KINNEY & LANGE BUILDING
312 South Third Street
Minneapolis, MN 55415-1002
Telephone: (612) 339-1863
Fax: (612) 339-6580

JDS:beh

This Page Blank (uspto)



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le **16 JUIN 1999**

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

This Page Blank (uspto)

REQUÊTE EN DÉLIVRANCE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : (1) 42.94.52.52 Télécopie : (1) 42.93.59.30

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES **15 JUIN 1998**

N° D'ENREGISTREMENT NATIONAL **98 07666 -**

DÉPARTEMENT DE DÉPÔT

DATE DE DÉPÔT **15 JUIN 1998**

**N. P. I.
RENNES**

**1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE**

**Patrice VIDON
Cabinet Patrice VIDON
Immeuble Germanium
80 avenue des Buttes de Coësmes
35700 RENNES**

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention

☐ demande divisionnaire



demande initiale

☐ certificat d'utilité

☐ transformation d'une demande
de brevet européen

☐ brevet d'invention

n° du pouvoir permanent : 4779 références du correspondant : 02.99.38.23.00

1

4779 02.99.38.23.00

☐ certificat d'utilité n°

date

Établissement du rapport de recherche

☐ différé

☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance

☐ oui

☐ non

Titre de l'invention (200 caractères maximum)

**Procédé et système pour payer à distance au moyen d'un radiotéléphone
mobile l'acquisition d'un bien et/ou d'un service.**

3 DEMANDEUR (S)

n° SIREN

code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

SFR Société Française du Radiotéléphone

Forme juridique

Société Anonyme

Nationalité (s)

Française

Adresse (s) complète (s)

**1, place Carpeaux
92915 PARIS LA DEFENSE CEDEX**

Pays

FRANCE

4 INVENTEUR (S) Les inventeurs sont les demandeurs

☐ oui

☒ non

En cas d'insuffisance de place, poursuivre sur papier libre

5 RÉDUCTION DU TAUX DES REDEVANCES

☐ requise pour la 1ère fois

☐ requise antérieurement au dépôt : joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine

numéro

date de dépôt

nature de la demande

7 DIVISIONS antérieures à la présente demande n°

date

n°

date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(nom et qualité du signataire - n° d'inscription)

**P. VIDON
(CEP 42-1258)**

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRES ENREGISTREMENT DE LA DEMANDE À L'INPI

DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DIVISION ADMINISTRATIVE DES BREVETS

26bis, rue de Saint-Petersbourg
75800 Paris Cédex 08
Tél. : (1) 42 94 52 52 - Télécopie : (1) 42 93 59 30

N° D'ENREGISTREMENT NATIONAL

780 7666

TITRE DE L'INVENTION :

Procédé et système pour payer à distance au moyen d'un radiotéléphone mobile l'acquisition d'un bien et/ou d'un service.

LE (S) SOUSSIGNÉ (S) **Patrice VIDON**
Cabinet Patrice VIDON
Immeuble Germanium
80 avenue des Buttes de Coësmes
35700 RENNES

DÉSIGNE (NT) EN TANT QU'INVENTEUR (S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

Mme Sophie FREY
55, rue de Paris
78100 SAINT-GERMAIN-EN-LAYE

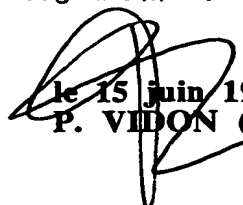
M. Arnaud CAPITANT
1, allée de la Brède
45650 ST JEAN-LE-BLANC

M. Christophe FRANCOIS
63, rue Jacques Dulud
92200 NEUILLY SUR SEINE

M. Philippe LUCAS
15, rue de l'Abbé Lambert
91200 PALAISEAU

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire


le 15 juin 1998
P. VIDON (CPI 92-1250)

Procédé et système pour payer à distance au moyen d'un radiotéléphone mobile l'acquisition d'un bien et/ou d'un service.

La présente invention concerne un procédé et un système pour payer à distance, au moyen d'un radiotéléphone mobile, l'acquisition d'un bien et/ou d'un service.

5 Divers procédés et systèmes de paiement électronique ont été proposés.

Le brevet EP 451 057 B1, publié le 9 octobre 1991, décrit un procédé et un système mettant en oeuvre un serveur de paiement. La solution préconisée dans ce brevet implique l'utilisation d'une carte émettant un signal vocal d'identification. Ce signal est reçu par le microphone du téléphone puis transmis au serveur de paiement.

10 La demande de brevet WO 96/32701 publiée le 17 octobre 1996 décrit également un procédé de paiement électronique mettant en oeuvre un serveur de paiement. Il permet d'effectuer des transactions liées à l'achat de biens offerts par des marchands au moyen de services télématiques via un réseau de télécommunication informatique ouvert, par exemple le réseau "Internet" sur lequel sont connectés des postes serveurs de marchands et des postes clients ainsi qu'un poste serveur de paiement.

15 Le paiement de biens ou de services à distance, au moyen d'un radiotéléphone mobile, via un réseau de télécommunication par liaison hertzienne, du type vocal GSM ou HDML, pose des problèmes de sécurité spécifiques à la nature de ces réseaux. Ces réseaux n'appartiennent pas à la catégorie des réseaux de télécommunication informatiques ouverts faisant l'objet de la solution préconisée par la demande WO 96/32701.

20 L'invention a pour but de fournir un procédé permettant de payer à distance, de manière sécurisée, au moyen d'un radiotéléphone mobile, un bien et/ou un service acquis par un acquéreur (qui n'est pas nécessairement le titulaire du radiotéléphone mobile) auprès d'un fournisseur. Le radiotéléphone mobile est interconnecté via une liaison hertzienne à un serveur de paiement raccordé à un réseau de télécommunication géré par un centre de gestion. Le procédé comprend les étapes ci-après définies.

25 Une première étape a pour objet d'identifier le titulaire du radiotéléphone mobile employé lors du règlement à distance au moyen d'un code d'identification confidentiel
30 contrôlé par le centre de gestion du réseau de télécommunication et/ou par le serveur de

paiement. Au terme de cette première étape, le gestionnaire du serveur de paiement est assuré que le titulaire du radiotéléphone mobile est régulièrement inscrit sur la liste des abonnés et fait licitement partie du réseau de télécommunication auquel le serveur de paiement est raccordé.

5 Une deuxième étape a pour objet d'authentifier l'acquéreur disposant du radiotéléphone mobile au moment du règlement au moyen d'un code de paiement confidentiel que l'acquéreur introduit dans le radiotéléphone mobile au moyen d'un clavier associé au radiotéléphone mobile. Le code de paiement confidentiel est contrôlé par le serveur de paiement. Au terme de cette deuxième étape, le gestionnaire du serveur
10 de paiement est assuré que l'acquéreur disposant du radiotéléphone mobile au moment du règlement est habilité à payer les biens et/ou les services acquis. Le gestionnaire du serveur de paiement peut alors autoriser ou faire procéder aux compensations entre le compte de l'acquéreur et celui du fournisseur.

15 Dans une autre variante de réalisation, le procédé selon l'invention comprend les étapes ci-après définies.

La première étape a pour objet, comme dans le cas de la précédente variante de réalisation, d'identifier le titulaire du radiotéléphone mobile employé lors du règlement à distance au moyen d'un code d'identification confidentiel contrôlé par le centre de gestion du réseau de télécommunication et/ou par le serveur de paiement. Au terme de cette étape
20 également, le gestionnaire du serveur de paiement est assuré que le titulaire du radiotéléphone mobile est régulièrement inscrit sur la liste des abonnés et fait licitement partie du réseau de télécommunication auquel le serveur de paiement est raccordé.

La deuxième étape a pour objet d'authentifier l'acquéreur disposant du radiotéléphone mobile au moment du règlement ainsi que la décision d'achat du bien et/ou du service acquis par l'acquéreur auprès du fournisseur au moyen d'une procédure
25 d'authentification. La procédure d'authentification comprend la génération d'une signature électronique au moyen d'un algorithme de sécurisation de paiement et/ou d'une ou plusieurs clés contenus dans des zones protégées du radiotéléphone mobile. La signature électronique est générée à partir de données relatives à la transaction, telles que
30 le contenu et/ou le prix, et d'identifiants relatifs à l'acquéreur notamment un code de

paiement confidentiel. Le code de paiement confidentiel est introduit dans le radiotéléphone mobile au moyen d'un clavier associé au radiotéléphone mobile. La signature électronique est transmise par le radiotéléphone mobile à un serveur de paiement et/ou à un centre de contrôle. La signature électronique est contrôlée par le serveur de paiement et/ou le centre de contrôle. Elle est tenue à la disposition de l'acquéreur et du fournisseur.

Au terme de cette étape, le gestionnaire du serveur de paiement est assuré que l'acquéreur disposant du radiotéléphone mobile au moment du règlement est habilité à payer les biens et/ou les services acquis. La signature électronique permet d'arbitrer les éventuelles contestations entre l'acquéreur et/ou le fournisseur et/ou le serveur de paiement.

De préférence, le procédé selon l'invention comprend en outre une étape ayant pour objet de crypter les données relatives au règlement de l'acquisition des biens et/ou des services, transmises par voie hertzienne au serveur de paiement. Grâce à cette opération de cryptage, la confidentialité de l'acquisition est assurée.

De préférence également, le procédé selon l'invention comprend en outre une étape ayant pour objet le contrôle de l'intégrité des données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne au serveur de paiement. Ainsi, un fraudeur n'a pas la possibilité de modifier les dites données.

L'invention concerne aussi un système pour payer à distance, de manière sécurisée, un bien et/ou un service acquis par un acquéreur auprès d'un fournisseur. Le système comprend un radiotéléphone mobile, utilisé par un titulaire, interconnecté via une liaison hertzienne à un serveur de paiement raccordé à un réseau de télécommunication géré par un centre de gestion. Le système comprend également des moyens d'identification pour identifier le titulaire du radiotéléphone mobile utilisé lors du règlement à distance. Les moyens d'identification comprennent des moyens d'initialisation pour initialiser le radiotéléphone mobile en comparant un code d'identification confidentiel, contenu dans une zone mémoire protégée du radiotéléphone mobile, à un code secret connu du titulaire. De préférence, ces zones protégées sont situées dans une carte à microprocesseur que l'on glisse dans le radiotéléphone mobile, la

carte SIM (Subscriber Identity Module), carte d'identité du titulaire du radiotéléphone mobile. Le code secret est introduit par le titulaire dans le radiotéléphone mobile au moyen d'un clavier. Les moyens d'identification comprennent également des moyens de contrôle du code d'identification confidentiel. Les moyens de contrôle sont mis en oeuvre par le centre de gestion du réseau de télécommunication et/ou par le serveur de paiement. Grâce à ces moyens d'identification, le gestionnaire du serveur de paiement est assuré que le titulaire du radiotéléphone mobile est régulièrement inscrit sur la liste des abonnés. Il fait licitement partie du réseau de télécommunication auquel le serveur de paiement est raccordé.

Le système selon l'invention comprend également des moyens d'authentification. Dans une première variante de réalisation ces moyens d'authentification ont pour objet d'authentifier l'acquéreur disposant du radiotéléphone mobile au moment du règlement. A cet effet, l'acquéreur introduit un code de paiement confidentiel, connu de lui seul, dans le radiotéléphone mobile au moyen d'un clavier associé au radiotéléphone mobile. Le serveur de paiement comporte des moyens de contrôle pour contrôler le code de paiement confidentiel. Grâce à ces moyens d'authentification, le gestionnaire du serveur de paiement est assuré que l'acquéreur disposant du radiotéléphone mobile au moment du règlement est habilité à payer les biens et/ou les services acquis. Le gestionnaire du serveur de paiement peut alors autoriser ou faire procéder aux compensations entre le compte de l'acquéreur et celui du fournisseur.

Dans une autre variante de réalisation, les moyens d'authentification ont pour objet d'authentifier l'acquéreur disposant du radiotéléphone mobile au moment du règlement ainsi que la décision d'achat du bien et/ou du service acquis par l'acquéreur auprès du fournisseur. A cet effet, les moyens d'authentification comprennent des moyens de calcul pour calculer une signature électronique. La signature électronique est calculée par les moyens d'authentification d'une première part, au moyen d'un algorithme de sécurisation de paiement et/ou une clé contenus dans des zones protégées du radiotéléphone mobile, notamment dans la carte SIM du radiotéléphone mobile. La signature électronique est calculée par les moyens d'authentification d'une seconde part, au moyen de données relatives à la transaction, telles que le contenu et/ou le prix, et

d'identifiants relatifs à l'acquéreur notamment un code de paiement confidentiel connu uniquement de l'acquéreur. Le radiotéléphone mobile comprend des moyens d'entrée de données, notamment un clavier, qu'utilise l'acquéreur pour entrer le code de paiement confidentiel connu de lui seul. Le radiotéléphone mobile comprend des moyens de transmission pour transmettre la signature électronique au serveur de paiement et/ou à un centre de contrôle. Le serveur de paiement et/ou ledit centre de contrôle comprennent des moyens de contrôle pour contrôler la signature électronique et des moyens de stockage pour stocker la signature électronique et la tenir à la disposition de l'acquéreur et du fournisseur. Grâce à ces moyens d'authentification, le gestionnaire du serveur de paiement est assuré que l'acquéreur disposant du radiotéléphone mobile au moment du règlement est habilité à payer les biens et/ou les services acquis. La signature électronique permet d'arbitrer les éventuelles contestations entre l'acquéreur et/ou le fournisseur et/ou le serveur de paiement.

De préférence, le système selon l'invention comprend en outre des moyens de cryptage pour crypter les données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne au serveur de paiement. Grâce à ces moyens de cryptage, la confidentialité de l'acquisition est assurée.

De préférence également, le système selon l'invention comprend en outre des moyens de traitement permettant le contrôle de l'intégrité des données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne au serveur de paiement.

Ainsi, un fraudeur n'a pas la possibilité de modifier les dites données.

L'invention concerne aussi un radiotéléphone mobile employé pour payer à distance, de manière sécurisée, un bien et/ou un service acquis par un acquéreur auprès d'un fournisseur. Le radiotéléphone mobile selon l'invention présente les caractéristiques du radiotéléphone mobile ci-dessus décrit, employé pour mettre en oeuvre le procédé ou le système selon l'invention. Le radiotéléphone mobile, utilisé par un titulaire, est interconnecté via une liaison hertzienne à un serveur de paiement raccordé à un réseau de télécommunication géré par un centre de gestion. Le radiotéléphone mobile comprend des moyens d'initialisation pour initialiser le radiotéléphone mobile en comparant un code

d'identification confidentiel contenu dans une zone mémoire protégée du radiotéléphone mobile, notamment dans la carte SIM du radiotéléphone mobile, à un code secret connu du titulaire et introduit par ce dernier dans le radiotéléphone mobile au moyen d'un clavier. Le radiotéléphone mobile comprend également des moyens d'authentification.

- 5 Dans une première variante de réalisation, ces moyens d'authentification ont pour objet d'authentifier l'acquéreur disposant du radiotéléphone mobile au moment du règlement au moyen d'un code de paiement confidentiel. Le code de paiement confidentiel est introduit dans le radiotéléphone mobile par l'acquéreur au moyen d'un clavier associé au radiotéléphone mobile. Des moyens de transmission par voie hertzienne transmettent
- 10 ledit code de paiement confidentiel à des moyens de contrôle du code de paiement confidentiel situés dans un centre de gestion et/ou dans un serveur de paiement. Ainsi, le gestionnaire du serveur de paiement est assuré que le titulaire du radiotéléphone mobile est régulièrement inscrit sur la liste des abonnés et fait licitement partie du réseau de télécommunication auquel le serveur de paiement est raccordé.
- 15 Dans une autre variante de réalisation, les moyens d'authentification ont pour objet d'authentifier l'acquéreur disposant du radiotéléphone mobile au moment du règlement ainsi que la décision d'achat du bien et/ou du service acquis par l'acquéreur auprès du fournisseur. A cet effet, les moyens d'authentification comprennent des moyens de calcul pour calculer une signature électronique. La signature électronique est calculée par les
- 20 moyens d'authentification d'une première part, au moyen d'un algorithme de sécurisation de paiement et/ou une clé contenus dans des zones protégées du radiotéléphone mobile, notamment dans la carte SIM du radiotéléphone mobile. La signature électronique est calculée par les moyens d'authentification d'une seconde part, au moyen de données relatives à la transaction, telles que le contenu et/ou le prix, et d'identifiants relatifs à
- 25 l'acquéreur notamment un code de paiement confidentiel connu uniquement de l'acquéreur. Le radiotéléphone mobile comprend des moyens d'entrée de données, notamment un clavier qu'utilise l'acquéreur, pour entrer le code de paiement confidentiel, connu de lui seul. Le radiotéléphone mobile comprend des moyens de transmission pour transmettre ladite signature électronique audit serveur de paiement et/ou à un centre de
- 30 contrôle. Grâce à ces moyens d'authentification, le gestionnaire du serveur de paiement

est assuré que l'acquéreur disposant du radiotéléphone mobile au moment du règlement est habilité à payer les biens et/ou les services acquis. La signature électronique permettra d'arbitrer les éventuelles contestations entre l'acquéreur et/ou le fournisseur et/ou le serveur de paiement.

5 De préférence, le radiotéléphone mobile selon l'invention comprend en outre des moyens de cryptage pour crypter les données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne au serveur de paiement. Grâce à ces moyens de cryptage, la confidentialité de l'acquisition est assurée.

10 De préférence également, le radiotéléphone mobile selon l'invention comprend en outre des moyens de traitement permettant le contrôle de l'intégrité des données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne au serveur de paiement. Ainsi, un fraudeur n'a pas la possibilité de modifier les dites données.

15 D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description de variantes de réalisation de l'invention, données à titre d'exemple indicatif et non limitatif, et de :

- la figure 1 qui représente une vue d'ensemble schématique d'un système selon l'invention ;
- la figure 2 qui représente une vue, sous la forme de bloc diagramme, d'un radiotéléphone ;
- la figure 3 qui représente une vue, sous la forme de bloc diagramme, d'un centre de gestion d'un réseau GSM ;
- la figure 4 qui représente une vue, sous la forme de bloc diagramme, d'un serveur de paiement ;
- la figure 5 qui représente sous forme d'organigramme les phases des opérations relatives à l'acquisition d'un bien ou d'un service.

On va maintenant décrire les figures 1 à 5.

30 Le système comprend un radiotéléphone 1 mobile, utilisé par un titulaire 2, interconnecté via une liaison hertzienne 3 à un serveur de paiement 4 raccordé à un réseau de télécommunication 5 géré par un centre de gestion d'abonnés 6. Dans le cas de la

variante de réalisation représentée sur la figure 1, l'acquéreur et le titulaire 2 sont une même personne. Dans d'autres variantes de réalisation, l'acquéreur pourrait être une personne distincte du titulaire. Le système permet à l'acquéreur 2 muni d'un radiotéléphone mobile 1 de payer à distance de manière sécurisée, un bien et/ou un service qu'il a acquis auprès d'un fournisseur 7 disposant d'un serveur de vente à distance 8. Le serveur de vente 8 est interconnecté par un réseau de communication 9 au centre de gestion d'abonnés 6. Le radiotéléphone mobile 1 comprend des moyens d'identification 20 situés dans le module de gestion de communication 21. Les moyens d'identification 20 permettent d'identifier le titulaire 2 du radiotéléphone mobile 1. Les moyens d'identification 20 comprennent des moyens d'initialisation 22 pour initialiser le radiotéléphone mobile 1 en comparant un code d'identification confidentiel contenu dans une zone mémoire protégée 23 du radiotéléphone mobile 1 à un code secret, connu du titulaire 2. Dans le cas de la variante de réalisation décrite en se référant à la figure 2, les zones protégées 23 sont situées dans une carte à microprocesseur que l'on glisse dans le radiotéléphone mobile. Cette carte est connue sous le nom de carte SIM (Subscriber Identity Module), elle est la carte d'identité du titulaire 2 du radiotéléphone mobile 1. Le code secret est introduit par le titulaire 2 dans le radiotéléphone mobile 1 au moyen d'un clavier 24. Les moyens d'identification 20 comprennent également des moyens de contrôle 25 du code d'identification confidentiel. Les moyens de contrôle 25 sont mis en oeuvre par le centre de gestion 6 et/ou par le serveur de paiement 4. En cas de comparaison positive entre le code secret et le code d'identification confidentiel, les moyens de contrôle 25 envoient un signal "contrôle d'identification validé" 50 vers le module de gestion des abonnés 30 du centre de gestion 6. Le module de gestion des abonnés 30 vérifie que le titulaire du radiotéléphone mobile 1 fait partie de la liste des abonnés et envoie un accusé de réception 51 vers le radiotéléphone mobile 1. Un message 52 de contrôle d'identification validé est également transmis vers le module identification 40 du serveur de paiement 4. Le radiotéléphone mobile 1 comporte également, de manière connue en soi, un écran afficheur 26, un haut parleur 27 et un microphone 28 interconnectés aux moyens de traitement de l'information 29. Les moyens d'émission et de réception radio 29a comprennent une antenne et sont connectés au module de

traitement de l'information 29.

Grâce à cette combinaison de moyens, le gestionnaire 4a du serveur de paiement 4 est assuré que le titulaire 2 du radiotéléphone mobile 1 est régulièrement inscrit sur la liste des abonnés 30. Il fait licitement partie du réseau de télécommunication auquel le serveur de paiement 4 est raccordé via le commutateur 31. Le commutateur 31 permet également de mettre en communication le système de communication par radiotéléphone mobile avec d'autres réseaux 32.

Le système selon l'invention comprend également des moyens d'authentification. Dans une première variante de réalisation, ces moyens d'authentification ont pour objet d'authentifier l'acquéreur 2 disposant du radiotéléphone mobile 1 au moment du règlement. A cet effet, l'acquéreur 2 introduit un code de paiement confidentiel, connu de lui seul, dans le radiotéléphone mobile au moyen du clavier 24 associé au radiotéléphone mobile 1. Le serveur de paiement 4 comporte un module de contrôle 41 pour contrôler le code de paiement confidentiel. Ce contrôle peut également être effectué par le centre de gestion des abonnés 6. Dans ce cas, le centre de gestion des abonnés comprend un module d'authentification 33 des titulaires de radiotéléphone abonnés au service de paiement à distance. Ce module d'authentification 33 contrôle le code de paiement confidentiel. Grâce à ces moyens d'authentification, le gestionnaire 4a du serveur de paiement 4 est assuré que l'acquéreur 2 disposant du radiotéléphone mobile 1 au moment du règlement est habilité à payer les biens et/ou les services acquis. Le gestionnaire du serveur de paiement peut alors autoriser ou faire procéder aux compensations entre le compte de l'acquéreur et celui du fournisseur.

Dans une autre variante de réalisation, les moyens d'authentification ont pour objet d'authentifier l'acquéreur 2 disposant du radiotéléphone mobile 1 au moment du règlement ainsi que la décision d'achat du bien et/ou du service acquis par l'acquéreur 2 auprès du fournisseur 7. La procédure d'authentification de l'acquéreur peut être mise en oeuvre avant ou après que l'acquéreur ait pris la décision d'achat. Dans l'exemple décrit en se référant à la figure 5, l'acquéreur 2 adresse une demande d'achat 53 au serveur de vente 8 du fournisseur 7. Il reçoit en retour les données relatives au prix du bien et/ou du service 54. L'acquéreur prend ensuite une décision d'achat 55. Dans le même temps, les

moyens de calcul 20a des moyens d'authentification 20b (le microprocesseur du radiotéléphone mobile) vont calculer une signature électronique. Cette signature électronique est calculée d'une première part, au moyen d'un algorithme de sécurisation de paiement et/ou d'une ou plusieurs clés contenues dans des zones protégées du radiotéléphone mobile 1 notamment dans la carte SIM 23 du radiotéléphone mobile 1. La signature électronique est calculée par les moyens d'authentification 20b d'une seconde part, au moyen de données relatives à la transaction, telles que le contenu et/ou le prix, et d'identifiants relatifs à l'acquéreur notamment un code de paiement confidentiel connu uniquement de l'acquéreur. Le radiotéléphone mobile 1 comprend des moyens d'entrée de données, notamment un clavier 24, qu'utilise l'acquéreur 2 pour entrer le code de paiement confidentiel, connu de lui seul. Le radiotéléphone mobile 1 comprend des moyens de transmission (des moyens d'émission et de réception radio 29a) pour transmettre (respectivement 55 et 56) la décision d'achat et la signature électronique au serveur 8 du fournisseur 7 et au serveur de paiement 4 et/ou à un centre de contrôle connecté au centre de gestion des abonnés 6. Le serveur de paiement 4 comprend un module de contrôle (ou de certification) 42 pour contrôler (pour certifier) la signature électronique. Ce module de contrôle 42 restitue le code de paiement en procédant aux opérations de calcul inverses de celles qui ont permis de calculer la signature électronique à partir du code de paiement. Le module de contrôle 42 procède à une vérification du code paiement. Si la transaction est acceptée par le serveur de paiement 4, un message 57 "transaction acceptée" est adressé au serveur du fournisseur, par le module accusé de réception 43 du serveur de paiement 4. Le serveur 8 du fournisseur adresse un message 58 de "confirmation d'achat" à l'acquéreur (au radiotéléphone mobile de l'acquéreur et/ou au domicile de l'acquéreur). Les signatures électroniques sont stockées par le module de stockage 44 du serveur de paiement 4 et sont tenues à la disposition de l'acquéreur et du fournisseur. Grâce à ces moyens d'authentification le gestionnaire 4a du serveur de paiement est assuré que l'acquéreur 2 disposant du radiotéléphone mobile 1 au moment du règlement est habilité à payer les biens et/ou les services acquis. La signature électronique permet d'arbitrer les éventuelles contestations entre l'acquéreur et/ou le fournisseur et/ou le serveur de paiement.

Les moyens de gestion de la communication et/ou les moyens de traitement de l'information 29 du radiotéléphone mobile 1 peuvent également comporter des moyens de cryptage 291 qui, en association avec les moyens de calcul 20a, permettent de crypter, de manière connue en soi, les données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne 3 au serveur de paiement 4. Grâce à ces moyens de cryptage, la confidentialité de l'acquisition est assurée.

Les moyens de traitement de l'information 29 du radiotéléphone mobile 1 peuvent également comporter des moyens de traitement 292 qui, en association avec les moyens de calcul 20a du microprocesseur, permettent, de manière connue en soi, le contrôle de l'intégrité des données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne 3 au serveur de paiement 4. Ainsi, un fraudeur n'a pas la possibilité de modifier les dites données.

Revendications

1. Procédé pour payer à distance, de manière sécurisée, au moyen d'un radiotéléphone mobile (1) utilisé par un titulaire (2), un bien et/ou un service acquis par un acquéreur auprès d'un fournisseur (7) ;

5 ledit radiotéléphone mobile étant interconnecté via une liaison hertzienne (3) à un serveur de paiement (4) raccordé à un réseau de télécommunication (5) géré par un centre de gestion (6) ;

ledit procédé comprenant les étapes :

- d'identifier (20) le titulaire (2) du radiotéléphone mobile (1) employé lors du règlement à distance au moyen d'un code d'identification confidentiel contrôlé par le centre de gestion (6) du réseau de télécommunication et/ou par le serveur de paiement (4),

(de telle sorte que le gestionnaire du serveur de paiement est assuré que le titulaire du radiotéléphone mobile est régulièrement inscrit sur la liste des abonnés et fait licitement partie du réseau de télécommunication auquel le serveur de paiement est raccordé),

- d'authentifier (20b) l'acquéreur (2) disposant du radiotéléphone mobile (1) au moment du règlement au moyen d'un code de paiement confidentiel que l'acquéreur introduit dans le radiotéléphone mobile au moyen d'un clavier (24) associé au radiotéléphone mobile (1), ledit code de paiement confidentiel étant contrôlé (41) par le serveur de paiement (4),

(de telle sorte que le gestionnaire du serveur de paiement est assuré que l'acquéreur disposant du radiotéléphone mobile au moment du règlement est habilité à payer les biens et/ou les services acquis et

de telle sorte que le gestionnaire du serveur de paiement peut autoriser ou faire procéder aux compensations entre le compte de l'acquéreur et celui du fournisseur).

2. Procédé pour payer à distance, de manière sécurisée, au moyen d'un radiotéléphone mobile (1) utilisé par un titulaire (2), un bien et/ou un service acquis par un acquéreur (2) auprès d'un fournisseur (7);

ledit radiotéléphone mobile (1) étant interconnecté via une liaison hertzienne (3) à un serveur de paiement (4) raccordé à un réseau de télécommunication (5) géré par un centre

de gestion (6) ;

ledit procédé comprenant les étapes :

- d'identifier (20) le titulaire (2) du radiotéléphone mobile employé lors du règlement à distance au moyen d'un code d'identification confidentiel contrôlé par le centre de gestion (6) du réseau de télécommunication et/ou par le serveur de paiement (4),

(de telle sorte que le gestionnaire du serveur de paiement est assuré que le titulaire du radiotéléphone mobile est régulièrement inscrit sur la liste des abonnés et fait licitement partie du réseau de télécommunication auquel le serveur de paiement est raccordé),

- d'authentifier (20b) l'acquéreur disposant du radiotéléphone mobile (1) au moment du règlement ainsi que la décision d'achat du bien et/ou du service acquis par l'acquéreur (2) auprès du fournisseur (7) au moyen d'une procédure d'authentification ;

ladite procédure d'authentification comprenant une signature électronique générée par un algorithme de sécurisation de paiement et/ou une clé contenus dans des zones (23) protégées du radiotéléphone mobile (1) notamment dans la carte SIM du radiotéléphone mobile,

ladite signature électronique étant générée (20a) à partir de données relatives à la transaction, telles que le contenu et/ou le prix, et d'identifiants relatifs à l'acquéreur notamment un code de paiement confidentiel ;

ledit code de paiement confidentiel étant introduit dans le radiotéléphone mobile (1) au moyen d'un clavier (24) associé au radiotéléphone mobile ;

ladite signature électronique étant transmise (29a) par le radiotéléphone mobile audit serveur de paiement et/ou à un centre de contrôle ;

ladite signature électronique étant contrôlée (42) par ledit serveur de paiement (4) et/ou ledit centre de contrôle et étant tenue (43, 44) à la disposition de l'acquéreur et du fournisseur,

(de telle sorte que le gestionnaire du serveur de paiement est assuré que l'acquéreur disposant du radiotéléphone mobile au moment du règlement est habilité à payer les biens et/ou les services acquis,

de telle sorte que la signature électronique permettra d'arbitrer les éventuelles contestations entre l'acquéreur et/ou le fournisseur et/ou le serveur de paiement).

3 . Procédé selon l'une quelconque des revendications 1 ou 2 comprenant en outre l'étape :

- 5 - de crypter (291) les données relatives au règlement de l'acquisition des biens et/ou des services, transmises par voie hertzienne au serveur de paiement,
(de telle sorte que la confidentialité de l'acquisition est assurée).

4 . Procédé selon l'une quelconque des revendications 1 à 3 comprenant en outre l'étape :

- 10 - de contrôler (292) l'intégrité des données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne au serveur de paiement,
(de telle sorte qu'un fraudeur n'a pas la possibilité de modifier les dites données).

5 . Système pour payer à distance, de manière sécurisée, un bien et/ou un service
15 acquis par un acquéreur (2) auprès d'un fournisseur (7) ;
ledit système comprenant :

- un radiotéléphone mobile (1), utilisé par un titulaire (2), interconnecté via une
liaison hertzienne (3) à un serveur de paiement (4) raccordé à un réseau de
télécommunication (5) géré par un centre de gestion (6);
20 - des moyens d'identification (20) pour identifier le titulaire du radiotéléphone
mobile utilisé lors du règlement à distance ; lesdits moyens d'identification
comprenant :

- * des moyens d'initialisation (22) pour initialiser le radiotéléphone mobile
(1) en comparant un code d'identification confidentiel contenu dans une
25 zone mémoire (23) protégée du radiotéléphone mobile (1) à un code
secret, connu du titulaire, et introduit par ce dernier dans le radiotéléphone
mobile au moyen d'un clavier (24),
 * des moyens de contrôle (25) du code d'identification confidentiel, lesdits
moyens de contrôle, étant mis en oeuvre par le centre de gestion (6) du
30 réseau de télécommunication et/ou par le serveur de paiement,

(de telle sorte que le gestionnaire du serveur de paiement est assuré que le titulaire du radiotéléphone mobile est régulièrement inscrit sur la liste des abonnés et fait licitement partie du réseau de télécommunication auquel le serveur de paiement est raccordé),

- des moyens d'authentification (20b) pour authentifier l'acquéreur (2) disposant du radiotéléphone mobile (1) au moment du règlement au moyen d'un code de paiement confidentiel que l'acquéreur (2) introduit dans le radiotéléphone mobile (1) au moyen d'un clavier (24) associé au radiotéléphone mobile, ledit serveur de paiement (4) comportant des moyens de contrôle (41) pour contrôler le code de paiement confidentiel,

(de telle sorte que le gestionnaire du serveur de paiement est assuré que l'acquéreur disposant du radiotéléphone mobile au moment du règlement est habilité à payer les biens et/ou les services acquis et

de telle sorte que le gestionnaire du serveur de paiement peut autoriser ou faire procéder aux compensations entre le compte de l'acquéreur et celui du fournisseur).

6. Système pour payer à distance, de manière sécurisée, un bien et/ou un service acquis par un acquéreur (2) auprès d'un fournisseur (7) ;

ledit système comprenant :

- un radiotéléphone mobile (1), utilisé par un titulaire (2), interconnecté via une liaison hertzienne (3) à un serveur de paiement (4) raccordé à un réseau de télécommunication (5) géré par un centre de gestion (6) ;

- des moyens d'identification (20) pour identifier le titulaire (2) du radiotéléphone mobile (1) utilisé lors du règlement à distance ; lesdits moyens d'identification comprenant :

* des moyens d'initialisation (22) pour initialiser le radiotéléphone mobile (1) en comparant un code d'identification confidentiel contenu dans une zone mémoire (23) protégée du radiotéléphone mobile, notamment dans la carte SIM du radiotéléphone mobile, à un code secret, connu du titulaire, et introduit par ce dernier dans le radiotéléphone mobile au moyen d'un clavier (24),

* des moyens de contrôle (25) du code d'identification confidentiel, lesdits

moyens de contrôle, étant mis en oeuvre par le centre de gestion (6) du réseau de télécommunication et/ou par le serveur de paiement (5),

(de telle sorte que le gestionnaire du serveur de paiement est assuré que le titulaire du radiotéléphone mobile est régulièrement inscrit sur la liste des abonnés et fait licitement
5 partie du réseau de télécommunication auquel le serveur de paiement est raccordé),

- des moyens d'authentification (20b) pour authentifier l'acquéreur disposant du radiotéléphone mobile (1) au moment du règlement ainsi que la décision d'achat du bien et/ou du service acquis par l'acquéreur (2) auprès du fournisseur (7) ;

lesdits moyens d'authentification comprenant des moyens de calcul (20a) pour calculer
10 une signature électronique ;

* ladite signature électronique étant calculée par lesdits moyens d'authentification (20a, 20b) d'une première part, au moyen d'un algorithme de sécurisation de paiement et/ou une clé contenus dans des zones protégées (23) du radiotéléphone mobile notamment dans la carte
15 SIM du radiotéléphone mobile (1),

* ladite signature électronique étant calculée par lesdits moyens d'authentification (20a, 20b) d'une seconde part, au moyen de données relatives à la transaction, telles que le contenu et/ou le prix, et d'identifiants relatifs à l'acquéreur notamment un code de paiement
20 confidentiel ;

ledit radiotéléphone mobile (1) comprenant des moyens d'entrée de données, notamment un clavier (24), pour entrer ledit code de paiement confidentiel ;

ledit radiotéléphone mobile (1) comprend des moyens de transmission (29a) pour transmettre ladite signature électronique audit serveur de paiement et/ou à un centre de
25 contrôle ;

ledit serveur de paiement et/ou ledit centre de contrôle comprenant des moyens de contrôle (42) pour contrôler ladite signature électronique et des moyens de stockage (44) pour stocker ladite signature électronique et la tenir (43) à la disposition de l'acquéreur et du fournisseur,

(de telle sorte que le gestionnaire du serveur de paiement est assuré que l'acquéreur
30

disposant du radiotéléphone mobile au moment du règlement est habilité à payer les biens et/ou les services acquis,

de telle sorte que la signature électronique permettra d'arbitrer les éventuelles contestations entre l'acquéreur et/ou le fournisseur et/ou le serveur de paiement).

- 5 7 . Système selon l'une des revendications 5 ou 6 comprenant en outre :
- des moyens de cryptage (291) pour crypter les données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne au serveur de paiement,
- (de telle sorte que la confidentialité de l'acquisition est assurée).*
- 10 8 . Système selon l'une quelconque des revendications 5 à 7 comprenant en outre :
- des moyens de traitement (292) permettant le contrôle de l'intégrité des données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne au serveur de paiement,
- (de telle sorte qu'un fraudeur n'a pas la possibilité de modifier les dites données).*
- 15 9 . Radiotéléphone mobile (1) employé pour payer à distance, de manière sécurisée, un bien et/ou un service acquis par un acquéreur (2) auprès d'un fournisseur (7) ;
- ledit radiotéléphone mobile (1), utilisé par un titulaire, étant interconnecté via une liaison hertzienne (3) à un serveur de paiement (4) raccordé à un réseau de télécommunication (5) géré par un centre de gestion (6) ;
- 20 ledit radiotéléphone mobile comprenant :
- des moyens d'initialisation (22) pour initialiser le radiotéléphone mobile en comparant un code d'identification confidentiel contenu dans une zone mémoire (23) protégée du radiotéléphone mobile, notamment dans la carte SIM du radiotéléphone mobile, à un code secret, connu du titulaire, et introduit par ce
- 25 dernier dans le radiotéléphone mobile au moyen d'un clavier (24),
- des moyens d'authentification (20b) pour authentifier l'acquéreur (2) disposant du radiotéléphone mobile (1) au moment du règlement au moyen d'un code de paiement confidentiel que l'acquéreur introduit dans le radiotéléphone mobile au moyen d'un clavier (24) associé au radiotéléphone mobile,
- 30 - des moyens de transmission (29a) par voie hertzienne transmettant ledit code de

paiement confidentiel à des moyens de contrôle (41) du code de paiement confidentiel situés dans un centre de gestion et/ou dans un serveur de paiement (4),

(de telle sorte que le gestionnaire du serveur de paiement est assuré que le titulaire du radiotéléphone mobile est régulièrement inscrit sur la liste des abonnés et fait licitement partie du réseau de télécommunication auquel le serveur de paiement est raccordé),

10. Radiotéléphone mobile (1) employé pour payer à distance, de manière sécurisée, un bien et/ou un service acquis par un acquéreur (2) auprès d'un fournisseur (7) ; ledit radiotéléphone mobile (1), utilisé par un titulaire (2), étant interconnecté via une liaison hertzienne (3) à un serveur de paiement (4) raccordé à un réseau de télécommunication (5) géré par un centre de gestion (6);

ledit radiotéléphone mobile comprenant :

- des moyens d'initialisation (22) pour initialiser le radiotéléphone mobile en comparant un code d'identification confidentiel contenu dans une zone mémoire (23) protégée du radiotéléphone mobile, notamment dans la carte SIM du radiotéléphone mobile, à un code secret, connu du titulaire, et introduit par ce dernier dans le radiotéléphone mobile au moyen d'un clavier (24),

(de telle sorte qu'après initialisation, le gestionnaire du serveur de paiement est assuré que le titulaire du radiotéléphone mobile est régulièrement inscrit sur la liste des abonnés et fait licitement partie du réseau de télécommunication auquel le serveur de paiement est raccordé),

- des moyens d'authentification (20b) pour authentifier l'acquéreur disposant du radiotéléphone mobile au moment du règlement ainsi que la décision d'achat du bien et/ou du service acquis par l'acquéreur auprès du fournisseur ;

lesdits moyens d'authentification comprenant des moyens de calcul (20a) pour calculer une signature électronique ;

* ladite signature électronique étant calculée par lesdits moyens d'authentification (20a, 20b) d'une première part, au moyen d'un algorithme de sécurisation de paiement et/ou une clé contenus dans des zones protégées (23) du radiotéléphone mobile notamment dans la carte

SIM du radiotéléphone mobile,

* ladite signature électronique étant calculée par lesdits moyens d'authentification (20a, 20b) d'une seconde part, au moyen de données relatives à la transaction, telles que le contenu et/ou le prix, et d'identifiants relatifs à l'acquéreur notamment un code de paiement confidentiel ;

ledit radiotéléphone mobile comprenant des moyens d'entrée de données, notamment un clavier (24), pour entrer ledit code de paiement confidentiel ;

ledit radiotéléphone mobile comprend des moyens de transmission (29a) pour transmettre ladite signature électronique audit serveur de paiement (4) et/ou à un centre de contrôle ;
(de telle sorte que le gestionnaire du serveur de paiement est assuré que l'acquéreur disposant du radiotéléphone mobile au moment du règlement est habilité à payer les biens et/ou les services acquis et,

de telle sorte que la signature électronique permettra d'arbitrer les éventuelles contestations entre l'acquéreur et/ou le fournisseur et/ou le serveur de paiement).

11. Radiotéléphone mobile selon l'une des revendications 9 ou 10 comprenant en outre :

- des moyens de cryptage (291) pour crypter les données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne au serveur de paiement,

(de telle sorte que la confidentialité de l'acquisition est assurée).

12. Radiotéléphone mobile selon l'une quelconque des revendications 9 à 11 comprenant en outre :

- des moyens de traitement (292) permettant le contrôle de l'intégrité des données relatives au règlement de l'acquisition des biens et/ou des services transmises par voie hertzienne au serveur de paiement,

(de telle sorte qu'un fraudeur n'a pas la possibilité de modifier les dites données).

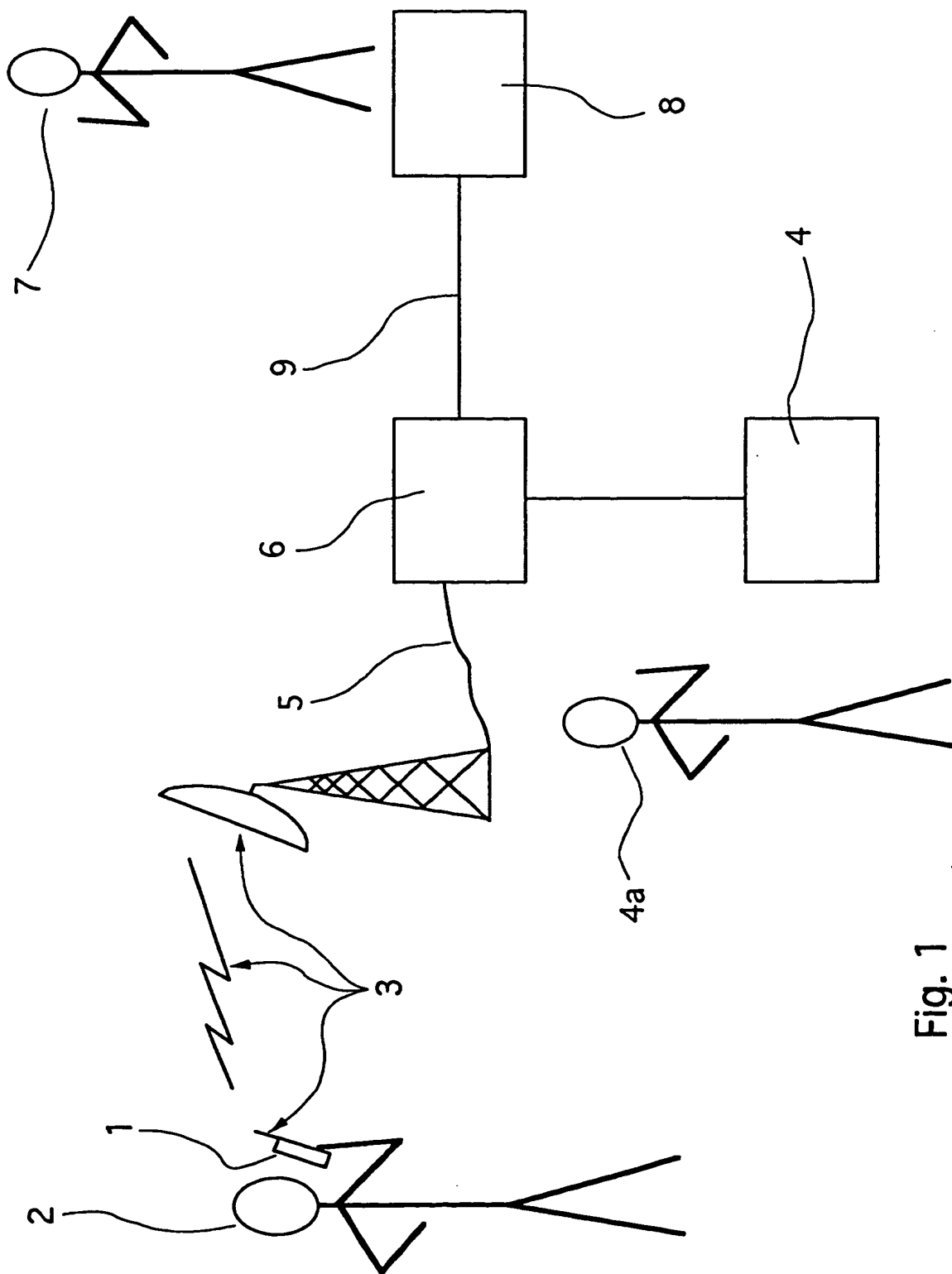


Fig. 1

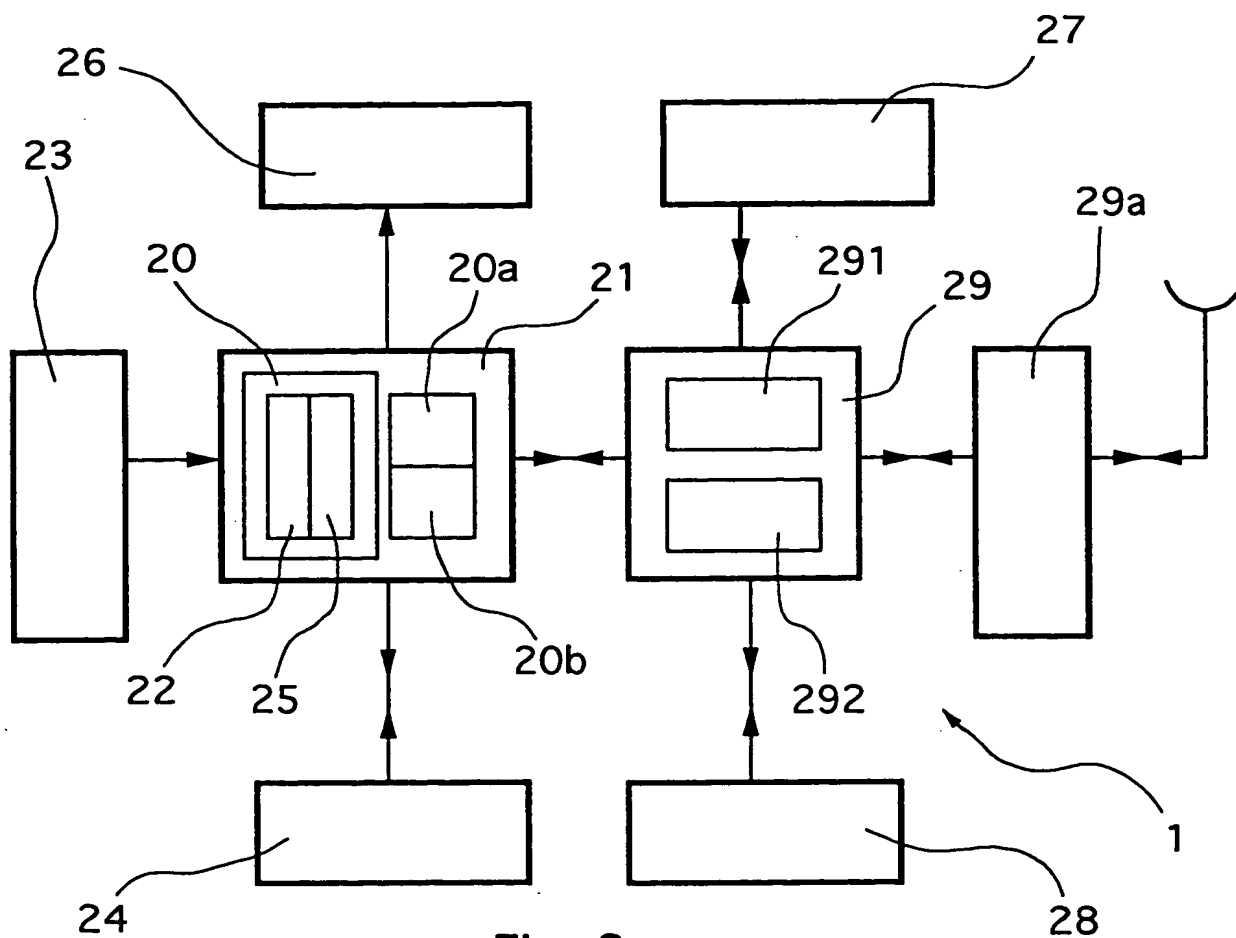


Fig. 2

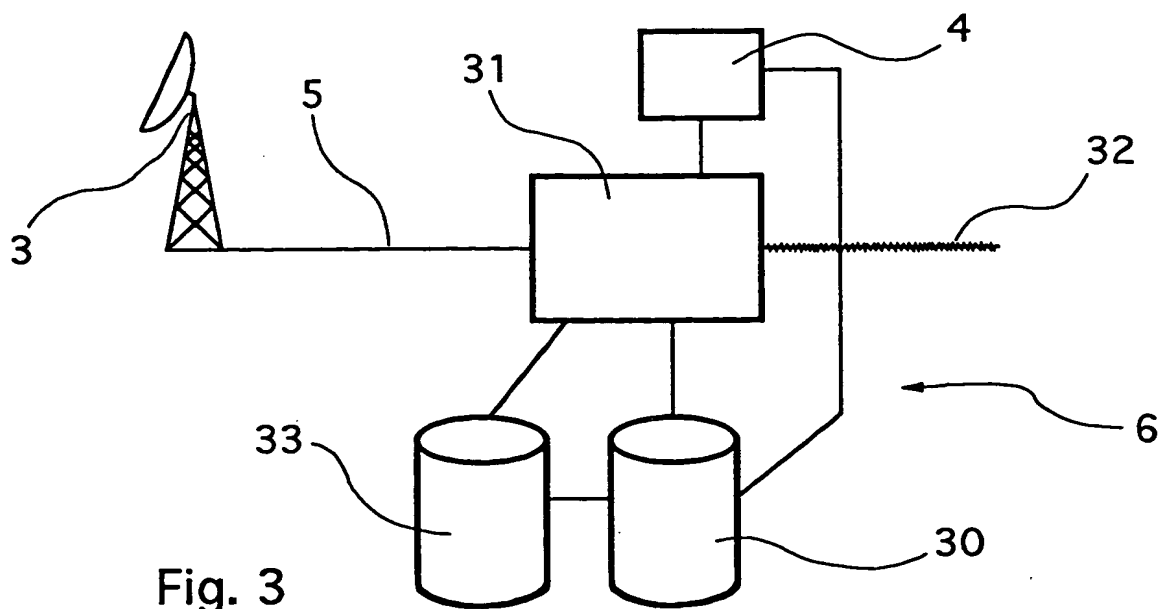


Fig. 3

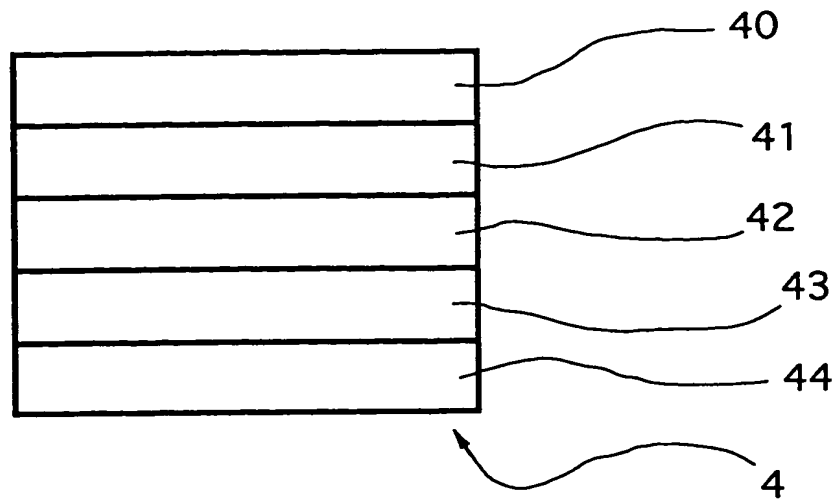


Fig. 4

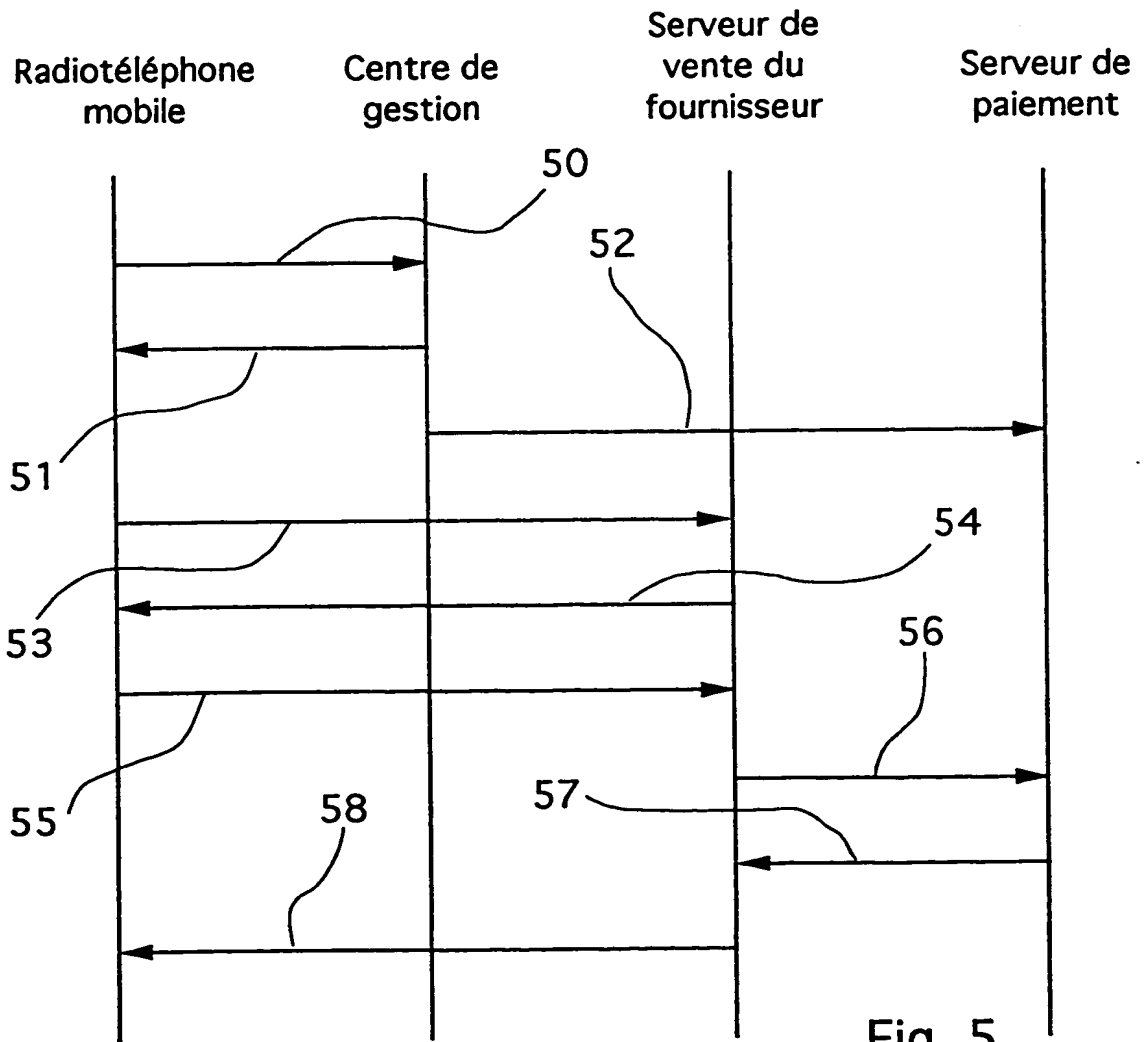


Fig. 5

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☒ **SKEWED/SLANTED IMAGES**
- ☒ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)